Random Graphs and Erdős Magic

Joel Spencer

Asperen, October 30- November 1, 2018

A Special Note: These notes are only an approximation to the actual lectures. There is some extra material here, and there will almost certainly be some material in the lectures not covered in the notes. In particular, the split into specific days should be regarded only as an estimate. – JS

The Probabilistic Method.
Lecture I: Tuesday, October 30

1 History

The probabilistic method prove the existence of some object with a given property, by showing that it occurs with non-zero probability when we select a random object from an appropriate probability space. Using the probabilistic method, we can prove theorems that themselves involve no probability. We can often avoid complicated constructions.

The probabilistic method was invented by Paul Erdős. It is hard to say that it was his chief discovery, as he has contributed so many things to many different branches of mathematics. But it is bears most deeply the mark of his character, and he nurtured it as its sole practitioner for 25 years.

The first theorem we will prove has a story associated with it that goes back to well before Erdős' development of the probabilistic method. Three friends were walking in the hills outside of Budapest, as was their habit, talking about mathematics: G. Szekeres, Esther Klein, and the 17 year old Paul Erdős, who was already know on the university campus as a mathematical sorcerer.[1] Esther had brought a mathematical problem back with her. Allthough they didn't realize it, Ramsey had already proven it, and it is now known as a (version) of Ramsey's theorem:

2 Ramsey's Theorem

Let K_n be the complete graph with n nodes.

[1]Soon after Erdős was dubbed Die Zauberer von Budapest

Theorem 2.1 *Ramsey's Theorem (limited version): For all k, l, there exists n so that the edges of K_n are colored red and blue, either there exists a red complete sub-graph of k points or there exists a blue complete sub-graph of l points.*

It turns out, Szekeres was able to prove this, and get a simple bound on the growth rate of n, though, at the time, he was majoring in chemical engineering. It may seem amazing that a chemical engineer could tackle this problem. In fact, as he was to recall in later years, he had a powerful incentive: he was married with Esther shortly afterwards.

For an example of Ramseys theorem with $k = l = 3$, the graph $n = 6$ is satisfactory. Consider, for instance six people sitting listening to this lecture. We'll call a person gregarious if they know at least 3 other people. (Let us assume that "knowing" is reflexive, as we are concerned with undirected graphs.) Suppose there is a gregarious person. If any two of people known also know each other, then we have a gregarious triangle. If all three of them are mutually unacquainted, then we have a complete subgraph of strangers. Obviously, if there is no gregarious person, then there must be a retiring person who doesn't know at least three people, and the argument works symmetrically.

Define *the Ramsey function* $R(k, l)$ is the least n with this property.

It can be shown by a simple induction that:

$$R(k, l) \leq \binom{k + l - 2}{k - 1}$$

(The method is to show $R(k, l) \leq R(k - 1, l) + R(k, l - 1)$.)

In 1946-47, Erdős proved both an upper and a lower bound for $R(k, k)$. The lower bound involved essentially the first use of the probabilistic method.[2]

Theorem 2.2 (Erdős 47) [3]

$$R(k, k) \leq \binom{2k - 2}{k - 1} \sim c4^k k^{-1/2}$$

Theorem 2.3 (Erdős 47) *If $\binom{n}{k}2^{1-\binom{k}{2}}$, then $R(k, k) > n$.*

We will prove this later theorem with the probabilistic method. In order to prove that Ramsey's function is greater than n, we must prove there exists a two-coloring χ of K_n with no mono χ of K_n (where *mono* is short for monochromatic, and "mono χ" means "monochromatic under χ").

To prove this, consider a random coloring on n points. (So the probability space contains $2^{\binom{n}{2}}$ "points"). For any $S \subseteq \{1, \ldots, n\}$, $|S| = k$, let A_S be the event that S is mono χ. Then:

$$\Pr[A_S] = 2^{1-\binom{k}{2}}$$

[2] There was another paper a bit earlier by Schütte that used something like the probabilistic method, but its significance was not appreciated.

[3] In this course, we will be interested in the asymptotic behavior. My recent book "Asymptopia" deals with this viewpoint.

Let BAD $= \bigvee_{|S|=k} A_S$. BAD is the event that there is a set of points that is mono. We are looking for a set that is not mono, so set GOOD $= \overline{\text{BAD}}$.

By the union bound, we have:

$$\Pr[\text{BAD}] \leq \sum_{|S|=k} \Pr[A_S] = \binom{n}{k} 2^{1-\binom{k}{2}} < 1$$

Therefore,

$$\Pr[\text{GOOD}] > 0$$

Thus, by "Erdős magic" we can conclude there is a good χ.[4] End of Proof.

Analysis

Now let us analyze this result, as Erdős did in his paper, to see what explicit asymptotic bound this gives for n. This is a typical example of what might be called "asymptotic calculus".

Define:

$$f(k) := \max n \text{ such that } \binom{n}{k} 2^{1-\binom{k}{2}} < 1$$

As a rough estimate, lets try:[5]

$$\binom{n}{k} \approx \frac{n^k}{k!}$$

Then, as a first cut, we get:

$$\frac{n^k}{k!} \approx 2^{k^2/2} \Rightarrow n \approx \sqrt{2}^k (\text{ignoring k!(!)})$$

Now, a little more formally, this can be converted into an upper bound:

$$\binom{n}{k} < \frac{n^k}{k!} < 2^{\binom{k}{2}-1}$$

$$n < k!^{1/k} 2^{\frac{1}{2}k-1} 2^{-\frac{1}{k}}$$

where $2^{-\frac{1}{k}} \sim 1$ asymptotically, and can be ignored. Now we can apply Stirling's formula to get an approximation for $k!$:

$$k! \sim k^k e^{-k} \sqrt{2\pi k} \Rightarrow (k!)^{\frac{1}{k}} \sim \frac{k}{e}$$

Plugging back in:

$$n < \frac{k}{e\sqrt{2}} \sqrt{2}^k$$

[4] This non-constructive proof leads to algorithmic questions: how long does it take to find a solution?

[5] Note that "$\approx$" means "roughly like", with no formal interpretation. $f(n) \sim g(n)$, on the other hand, means $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$.

We saw the $\sqrt{2}^k$ term when we dropped $k!$, so we can conclude that n is at least exponential in k. In fact, we have a lower bound for n that turns out to be just the same:

$$\binom{n}{k} > \frac{(n-k)^k}{k!} \sim \frac{n^k}{k!} \text{if } \left(1 - \frac{k}{n}\right)^k \sim 1$$

This condition is fulfilled whenever $n >> k^2$ (if not, we have an additional $e^{-\frac{k^2}{n}}$ term). So certainly, with $n > ck2^{\frac{1}{k}}$, $\binom{n}{k} \sim \frac{n^k}{k!}$. Therefore

$$f(k) \sim \frac{k}{e\sqrt{2}}\sqrt{2}^k$$

End of Proof.
Remark: what is the intuition behind using randomness? We want a set that does *not* have structure, because structure can be used against us. Randomness is a way to get such a set.

3 Tournaments (Beginning)

A tournament T_n is a round-robin competition between n players (vertices). For all i, j, either i beats j or j beats i (directed edges).
Definition (Schütte) T_n has property S_k if for all distinct players $x_1, \ldots, x_k$ there exists y who beats all of them.

Some examples: S_1 - every player is beaten by all others. T_3 provides an example 1 beating 2 beating 3 beating 1. T_7 provides an example of a tournament with property S_2 The rule for the edges is: i beats j if $i-j$ is a square mod 7. What about S_{10}? This problem seems to get pretty complex as it scales up. Nevertheless, Erdős came up with a simple proof for the existence of tournaments using the probabilistic method.

Theorem 3.1 (Erdős, 1963) *For all k there exists a (finite) tournament T_k with property S_k.*

In fact, well show the following result, where we'll fill in the ... later!

Theorem 3.2 *(Erdős 1963) If ...... then there exists a tournament T_n with n vertices that has the property S_k.*

Proof: Consider a random tournament T_n. Let $K = \{x_1, \ldots, x_k\}$ be a set of k players. Call y is a witness for K if y beats $\{x_1, \ldots, x_k\}$. Then:

$$\Pr[y \text{ is a witness for } K] = 2^{-k}$$

Then let A_K be the event that K has no witness.

$$\Pr[A_K] = (1 - 2^{-k})^{n-k}$$

Why? Each $y \notin K$ has probability 2^{-k} of being a witness and therefore probability $1 - 2^{-k}$ of not being a witness. As different $y \notin K$ involve separate coin flips, the events "y is not a witness for K" are mutually independent.

Now, let $BAD = \bigvee_{|K|=k} A_K$ and $GOOD = \overline{BAD}$. Clearly, $GOOD$ is the event that the tournament has the property S_k.

Computing the probability of the event BAD is not easy. However, we can bound this probability using the fact that the probability of a disjunction of events is less than or equal to the sum of the probabilities of individual events. Therefore,

$$\Pr[BAD] \leq \sum_{|K|=k} \Pr[A_K] = \binom{n}{k}(1-2^{-k})^{n-k}.$$

Therefore, if we replace "......" in the statement of the theorem by the condition $\binom{n}{k}(1-2^{-k})^{n-k} < 1$, we will obtain $\Pr[GOOD] > 0$. Now,

> **Erdős Magic:** If the probability of an event is positive, there exists some point of the probability space for which the event occurs. For example, since $\Pr[GOOD] > 0$, there exists some tournament T_n with the property S_k.

End of Proof.

The first corollary of the above theorem is that for every k, there are tournaments with property S_k. The reason is that for every fixed k, $\binom{n}{k}$ is a polynomial in n, while $(1-2^{-k})^{n-k}$ is exponentially small. Therefore, the condition $\binom{n}{k}(1-2^{-k})^{n-k} < 1$ is satisfied if n is large enough.

Now, let $f(k)$ be the smallest n such that $\binom{n}{k}(1-2^{-k})^{n-k} < 1$. What are the asymptotics for $f(k)$?

In order to find the asymptotics, we estimate $\binom{n}{k}$ using the inequality $\binom{n}{k} \leq n^k$. This is not a good estimate in general (For example, $\frac{n^k}{k!}$ is a better estimate), but it turns out that in this problem using more accurate estimates won't give us better results. Also, we know that for small ϵ, we have $1-\epsilon \sim e^{-\epsilon}$, and for all positive ϵ, $1-\epsilon < e^{-\epsilon}$. Therefore, it suffices to have $n^k e^{-2^{-k}(n-k)} < 1$. Also, it turns out that we won't lose much by replacing $(n-k)$ by n. Therefore, we need $n^k < e^{2^{-k}n}$, or equivalently $2^k k \log n < n$.

Now, the problem is to find the smallest n such that $\alpha \log n < n$, where $\alpha = 2^k k$. If $n = \alpha \log \alpha (1+\epsilon)$ for some positive ϵ, we have

$$\alpha \log n = \alpha \log(\alpha \log \alpha (1+\epsilon)) = \alpha \log \alpha + \alpha \log((1+\epsilon)\log \alpha) < \alpha \log \alpha (1+\epsilon) = n.$$

Thus, for $n = \alpha \log \alpha (1+o(1))$, we have $\alpha \log n < n$. Therefore,

$$f(k) = (2^k k)\log(2^k k)(1+o(1)) = 2^k k^2 \ln 2(1+o(1)).$$

Therefore, if $ANS(k)$ denotes the minimum n for which there is a tournament T_n with the property S_k, we have $ANS(k) = O(k^2 2^k)$. The following theorem provides a lower bound for $ANS(k)$.

Theorem 3.3 *If $n \leq 2^k - 1$, then every tournament T_n with n vertices does not have the property S_k.*

Proof: It is easy to see that there must be a player in the tournament that wins at least half its games. Let x_1 be such a player, and A_1 be the set of players that have beaten x_1. Therefore, $|A_1| \le 2^{k-1} - 1$. Now consider a player x_2 in A_1 that wins at least half its games with other players in A_1, and let A_2 be the set of players in A_1 that have beaten x_2 (Thus, $|A_2| \le 2^{k-2}-1$). Similarly, we can define $x_3, x_4, \ldots$. Now, it is not difficult to see that the set $x_1, x_2, \ldots$ is a set of at most k players with no witness. End of Proof.

Using a more complicated non-probabilistic argument it can be shown that $ANS(k) = \Omega(k2^k)$. The exact asymptotic for $ANS(k)$ is not known.

Asymmetric Ramsey Numbers

Let's assume we want to find $R(1000, 2000)$. Therefore, we need to construct a 2-coloring of the edges of a complete graph with no red K_{1000} or blue K_{2000}. Since the situation is not symmetric between red and blue, we should not use a fair coin for coloring. Instead, we should bias the coin to color more edges with blue. Since we don't know how to bias the coin, we use a technique called *parameterization.*

To bound $R(k,l)$ (from below), try a coloring of K_n with $\Pr[\chi(\{i,j\}) = \text{Red}] = p$, where p is number that will be fixed later. There are two kinds of bad events: For every set S with $|S| = k$, A_S is the event that all the edges between the vertices in S are colored red, and for every set T with $|T| = l$, B_T is the event that all the edges between the vertices in T are colored blue. Let $BAD = \bigvee_{|S|=k} A_S \vee \bigvee_{|T|=l} B_T$.

Clearly, $\Pr[A_S] = p^{\binom{k}{2}}$ and $\Pr[B_T] = (1-p)^{\binom{l}{2}}$. Therefore,

$$\Pr[BAD] \le \binom{n}{k} p^{\binom{k}{2}} + \binom{n}{l} (1-p)^{\binom{l}{2}}.$$

Thus, we have proved the following theorem.

Theorem 3.4 *If there exists a $p \in [0,1]$ with $\binom{n}{k} p^{\binom{k}{2}} + \binom{n}{l}(1-p)^{\binom{l}{2}} < 1$, then $R(k,l) > n$.*

4 Alteration

Theorem 4.1 *For all integer m and $p \in [0,1]$*

$$R(k,l) \ge m - \binom{m}{k} p^{\binom{k}{2}} - \binom{m}{l} (1-p)^{\binom{l}{2}}$$

Proof: Take a random coloring of K_m with edges Red with probability p. For each red K_k and each blue K_l remove one of their vertices. The remaining graph will have neither red K_k nor blue K_l. As the expected number of points removed (we may remove the same point more than once but this just goes in our favor) is

$$\binom{m}{k} p^{\binom{k}{2}} + \binom{m}{l} (1-p)^{\binom{l}{2}}$$

so the expected number of points remaining is at least

$$m - \binom{m}{k} p^{\binom{k}{2}} - \binom{m}{l} (1-p)^{\binom{l}{2}}$$

and by Erdős Magic this can be achieved.

Asymptotic Calculus: How good does this theorem do? That is, given k, l, what is the maximum over m, p of

$$m - \binom{m}{k} p^{\binom{k}{2}} - \binom{m}{l} (1-p)^{\binom{l}{2}}$$

Lets take $k = 4$ and l large. We have

$$\binom{m}{l} (1-p)^{\binom{l}{2}} \le [me^{-pl/2}]^l$$

so this will be small if we take, say, $l = (3/p) \ln m$. We want $m - \binom{m}{4} p^6$ to be big. If we take $p = m^{-1/2}$ then we are subtracting less than $m/2$ so we still have at least $m/2$. That is, we would want $l = 3m^{1/2} \ln m$ or $m = cl^2 / \ln^2 l$. So the Theorem gives $R(4, l) = \Omega(l^2 \ln^{-2} l)$. This isn't the best known but its not bad.

2-Colorable Families

Let $\{A_1, A_2, \ldots, A_m\}$ be a family of subsets of a set Ω. We say that this family is *2-colorable* (or has the property B), if there is a coloring $\chi : \Omega \mapsto \{\text{Red}, \text{Blue}\}$ such that no A_k is monochromatic.

For example, the family $\{\{1,2\},\{2,3\},\{3,1\}\}$ is not 2-colorable Also, the family $\{\{1,2,3\}, \{1,5,6\}, \{3,4,5\}, \{1,4,7\}, \{3,6,7\},\{2,5,7\}, \{2,4,6\}\}$ is not 2-colorable. This family is constructed from the Fano projective plane

Theorem 4.2 *(Erdős 1963) Let $|A_i| = n$ for $1 \le i \le m$. If $m < 2^{n-1}$, then $\{A_1, \ldots, A_m\}$ is 2-colorable.*

Proof: Color randomly. Let BAD_i be the event that A_i is monochromatic. Since $|A_i| = n$, $\Pr[BAD_i] = 2^{1-n}$. Let $BAD = \bigvee_i BAD_i$. Therefore, $\Pr[BAD] \le m2^{1-n} < 1$. Therefore, there is a coloring which is not BAD, i.e., no A_i is monochromatic under this coloring. End of Proof. Let $m(n)$ be the least n such that there is a family $\{A_1, \ldots, A_m\}$ with $|A_i| = n$ which is not 2-colorable. Using this notation, the above theorem can be stated as follows.

Theorem 4.3 *(Erdős 1963) $m(n) \ge 2^{n-1}$.*

In order to find an upper bound for $m(n)$, we need to construct families that are not 2-colorable. The following non-probabilistic construction gives such a family. Set $|\Omega| = 2n - 1$, and consider the family of all n-element subsets of Ω. This family is not 2-colorable, because for every 2-coloring of Ω, there is a set of n elements that are colored the same. This shows that

$$m(n) \le \binom{2n-1}{n} \sim c4^n n^{-1/2}.$$

In most problems, the probabilistic method can be applied to find lower bounds or upper bounds, but not both. However, in this problem Erdős also used the probabilistic method to improve the above upper bound.

The idea is to pick the sets $A_1, A_2, \ldots, A_m$ independently at random from the set of all n-element subsets of a universe Ω of size v, where v is a parameter.

Let $\chi : \Omega \mapsto \{\text{Red}, \text{Blue}\}$ be a 2-coloring of the universe with a red and $b = v - a$ blue points. It is easy to see that

$$\Pr[A_i \text{ is monochromatic under } \chi] = \frac{\binom{a}{n} + \binom{b}{n}}{\binom{v}{n}} \ge \frac{2\binom{v/2}{n}}{\binom{v}{n}}.$$

The last inequality follows from the convexity of the function $\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}$ (this function is defined for all real x) for $x \ge n$.

Let BAD_χ be the event that no A_k is monochromatic under χ. Since A_k's are chosen independently, we have

$$\Pr[BAD_\chi] = \left(1 - \frac{\binom{a}{n} + \binom{b}{n}}{\binom{v}{n}}\right)^m \le \left(1 - \frac{2\binom{v/2}{n}}{\binom{v}{n}}\right)^m.$$

Let $BAD = \bigvee_\chi BAD_\chi$ and $GOOD = \overline{BAD}$. By the union bound, since there are 2^v different colorings,

$$\Pr[BAD] \le 2^v \left(1 - \frac{2\binom{v/2}{n}}{\binom{v}{n}}\right)^m.$$

Therefore, we have proved the following theorem.

Theorem 4.4 *(Erdős 1964) If there exists v with*

$$2^v \left(1 - \frac{2\binom{v/2}{n}}{\binom{v}{n}}\right)^m < 1,$$

then $m(n) > m$, i.e., there is a family $A_1, A_2, \ldots, A_m \subset \{1, \ldots, v\}$ with no 2-coloring.